



Australian Taxation Office scam preys on those still awaiting refunds

Blog Post by Paul Ducklin, Sophos

An alert Naked Security reader reported yet another taxation scam this morning, this time against the Australian Taxation Office (ATO). The personal income tax year in Australia ends on 30 June, and tax returns are generally due by the end of October. Refunds - at least for those with regular tax affairs and who have money owing - will typically have been processed and paid out by now. That doesn't stop the scammers, of course. They operate either in blissful ignorance of their victims' tax years, or add a few weasel-words about "delays", as a sort of general-purpose excuse for what might otherwise seem like an untimely message. To access your tax refund, please follow the steps below:- download the Tax Refund Form attached to this email- open it in a browser- follow the instructions on your screen. A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline. This scam, like many others of this sort, tries to avoid inviting you to click on a link and enter your details. This is something Australian financial institutions regularly and repeatedly advise that they will not ask you to do. Instead, you're invited to save an HTML attachment on your hard disk (i.e. to make a local copy of a web page) and to open it in your browser. This produces a form which is submitted, if you complete it and click Continue, to a hacked server in the USA. You might think that a web page which presents a form from one location (in this case, your hard disk) but submits the results to a completely different site would raise a warning, at least at an Internet Explorer security setting of "High". But it does not, presumably because this behaviour is considered unexceptional on legitimate sites. In other words, you need to be on guard yourself. In this example: Downloading and opening any sort of attachment from an unsolicited email is a Very Bad Idea. Requesting a tax refund on the say-so of an unsolicited email is a Very Bad Idea. Submitting your credit card details via an insecure (non-HTTPS) URL is a Very Bad Idea. The ATO has an official domain name of ato.gov.au, not ato.com.au. In other words, even if you're expecting a tax refund any day now, you should know better than to react to emails of this sort. Remember: don't buy, don't try, don't reply. If you simply don't play the game, the scammers lose.